> service's signature 742 and optionally various dispatch information elements from which it has been generated (there is no need to provide the message 702 and address 704 since they are already with the sender 701), thus the certificate 740 is typically tiny.

Further support for claim 159 is found in the specification as specified below:

page 32, lines 23-32 relating to FIG. 7:

> The certificate 740, which comprises the service's digital signature for the dispatch transaction, constitutes an non-repudiable evidence witnessed by the service for the dispatch and its contents, since the dispatched message contents is securely associated with the dispatch information (by means of the service's generated signature and/or fingerprint), and since the signature, the message and the dispatch information can at any later time be authenticated and verified by any third party both for integrity and originality by means of the service's public key....

Page 11, lines 16-26 relating to Fig. 1:

> When it is desired to authenticate the dispatch of the original documents (and possibly also their receipt at the destination 30), either the sender or the document dispatching service provides the associated authentication information, for example the envelope 32, unopened, to the party which required the authentication. When the envelope 32 is opened, it has associated therewith copies of both the dispatched documents and the dispatch information. The envelope 32 therefore, provides a reliable proof that the original documents 12 were dispatched on the date and to the destination listed on or in envelope 32.

Page 12, lines 1-3:

> The authentication-information could be provided by the service, directly to the court of law.

Claims 160 and 161 are directed to the authentication/verification phase independent of the process of generating the authentication data. Support for these two claims is found at page 26, lines 30-36:

> In accordance with one embodiment of the present invention, the authenticator further comprises a verification mechanism for verifying the authenticity of a set of information elements purported to be identical to the original set of information elements. It is however appreciated that the verification mechanism can be separated therefrom.

Further support is found at page 27, line 1 to page 29, line 13 regarding various verification mechanisms, and page 32, line 23 to page 33, line 7 regarding verification of a digital signature generated according to Fig. 7.

Respectfully submitted,

By: _____

Y. Kurt Chang - Reg. No. 41,397
One of the Attorneys for Applicants
LEYDIG, VOIT & MAYER, LTD.
Two Prudential Plaza, Suite 4900
180 North Stetson
Chicago, Illinois 60601-6780
(312) 616-5600